PCT/IB 03 / 06267
19. 12. 03

Europäisches Patentamt

European Patent Office

Office européen des brevets

REC'D 14 JAN 2004
WIPO PCT

Bescheinigung

Certificate

Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Best Available Copy

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03100032.6

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03100032.6
Demande no:

Anmeldetag:
Date of filing: 10.01.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Philips Corporate Intellectual Property GmbH
Habsburgerallee 11
52064 Aachen
ALLEMAGNE
Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Verfahren zur Konstruktion kryptographisch geeigneter hyperelliptischer Kurven

In Anspruch genommene Prioriät(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G09C1/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT SE SI SK TR LI

BESCHREIBUNG

Verfahren zur Konstruktion kryptographisch geeigneter hyperelliptischer Kurven

Der sichere Informationsaustausch über öffentliche Netze zwischen Sendern und Empfängern erfordert in vielen Fällen eine Verschlüsselung der auszutauschenden Nachrichten und Dokumente und ein Authentifikationverfahren für Sender und Empfänger.

Ein besonders häufig anzutreffendes Verschlüsselungs- oder kryptographisches Verfahren ist die sogenannte "asymmetrische" Verschlüsselung, die auch als "public-key" Verfahren bekannt ist. Diese Verfahren erlauben dem Empfänger einer Nachricht, dem Sender einen Schlüssel über das öffentliche Netz, d.h. im Prinzip jedem Dritten zugänglich, zu übermitteln. Dieser Schlüssel ist der öffentliche Schlüssel oder "public key". Der Sender verschlüsselt dann die Nachricht mit diesem Schlüssel. Die Leistungsfähigkeit der public-key Verfahren besteht darin, dass die solchermaßen verschlüsselte Nachricht nicht mit Kenntnis des öffentlichen Schlüssels allein wieder entschlüsselt werden kann. Nur der Erzeuger des öffentlichen Schlüssels, d.h. der Empfänger, kann die mit seinem öffentlichen Schlüssel verschlüsselte Nachricht entschlüsseln. Diese asymmetrische Verschlüsselung existiert in einer Reihe von Varianten. Das sicherlich verbreiteteste Beispiel eines asymmetrischen Verfahren ist die RSA Methode.

Eine Untergruppe der public-key Verfahren beinhaltet den Schritt der Exponentierung einer sehr großen natürlichen oder ganzen Zahl modulo einer weiteren großen natürlichen Zahl, dem öffentlichen Schlüssel. Die Sicherheit dieser Gruppe von Verfahren basiert auf der praktischen Unmöglichkeit, diskrete Logarithmen zu berechnen, um so den geheimen Exponenten zu erhalten. Beispiele der auf dem diskreten Logarithmusproblem aufbauenden Verschlüsselungs- und Authentifikationsverfahren sind unter den Namen Diffie-Hellman Verschlüsselung, El-Gamal Verschlüsselung und DSS Signaturen sowie Schnorr's Verfahren bekannt.

Die Auswahl der dem diskreten Logarithmus zugrundeliegenden endlichen Abelschen Gruppe kann auf verschiedene Weise geschehen. Eine mögliche Wahl ist die Gruppe der F_q-rationalen Elemente der Divisorklassengruppe vom Grad Null (0) einer hyperelliptischen Kurve, die über einem endlichen Körper F_q definiert ist. Für diese Gruppe, die auch F_q-rationale Punktegruppe der Jacobische Varietät der hyperelliptischen Kurve bezeichnet wird, existiert eine kompakte Darstellung der Gruppenelemente und ein effizienter Additionsalgorithmus. Weitere Einzelheiten zur Darstellung und Anwendung dieser Gruppe werden beispielsweise in N. Koblitz, „Algebraic Aspects of Cryptology", Springer-Verlag, 1998, erörtert.

Ein Problem bei dieser Wahl ist jedoch die Bestimmung einer geeigneten hyperelliptischen Kurve. Um die praktische Unlösbarkeit des diskreten Logarithmusproblems zu gewährleisten, sollte die Divisorklassengruppe dieser Kurve einen sehr großen Primfaktor enthalten, da die Laufzeit von Algorithmen zur Lösung des Logarithmusproblems von der Wurzel dieses Primfaktors abhängt. Wird die Leistung heutiger Rechenanlagen zugrundegelegt, sollte der Primfaktor mindestens 2^{160} Bit lang sein. Um die Effizienz des Systems zu gewährleisten, sollten jedoch die Parameter des Systems, wie zum Beispiel die Schlüssel, nicht zu groß werden.

Hyperelliptische Kurven, die diese Bedingungen erfüllen, sind Kurven, deren Divisorklassengruppe vom Grad Null eine prime oder fast prime Gruppenordnung aufweist. Um solche Kurven zu bestimmen, ist es im Prinzip möglich, die Koeffizienten der Kurve beliebig aus dem endlichen Körper F_p auszuwählen. Falls die resultierende Kurve nicht-singulär ist, kann dann die Zahl der Elemente der Divisorklassengruppe vom Grad Null bestimmt werden. Bisher ist jedoch ist noch kein Algorithmus gefunden worden, der diese Zahl, d.h. die Ordnung der Divisorklassengruppe, für eine zufällig bestimmte hyperelliptische Kurve über einem Körper mit großer Charakteristik ($p > 2^{80}$ für Kurven vom Geschlecht 2) ermittelt. Da zudem nur ein Bruchteil der hyperelliptischen Kurven eine Divisorklassengruppe mit primer oder fast primer Ordnung besitzt, bliebe selbst bei Existenz eines solchen Algorithmus das Problem bestehen, viele Kurven testen zu müssen, bevor eine im oben definierten Sinne sichere

Kurve bestimmt werden kann. Diese Tests gingen zu Lasten der Geschwindigkeit des Auswahlverfahrens.

Es ist wird daher als eine Aufgabe der Erfindung gesehen, ein Verfahren zur schnellen Bestimmung sicherer hyperelliptischer Kurven zu beschreiben.

Diese Aufgabe wird im Sinne der vorliegenden Erfindung dadurch gelöst, dass geeignete hyperelliptische Kurven unter Verwendung der Methode der komplexen Multiplikation konstruiert werden. Das erfinderische Verfahren erzeugt für kryptographische Anwendungen geeignete hyperelliptische Kurven vom Geschlecht 2 über endlichen Körpern mit großer Charakteristik.

Eine hyperelliptische Kurve vom Geschlecht g über einem Körper F_q (oder F_p) der Charakteristik ungleich 2 kann definiert werden als eine nicht-singuläre Kurve der Form

$$y^2 = f(x),$$

wobei f(x) ein normiertes Polynom vom Grade 2g+1 ist.

Die komplexe Multiplikationsmethode, im folgenden als CM-Methode bezeichnet, ist als solche bekannt und wurde z.B. von Atkin zur Konstruktion von elliptischen Kurven benutzt. Für Einzelheiten dieser bekannten Anwendung der CM-Theorie sei verwiesen auf: A.O.L. Atkin, F. Morain, Elliptic curves and primality proving, Math. Comp. 61:29-68, 1993. Die bekannte CM-Methode erlaubt es, zu einer gegebenen imaginär quadratischen Ordnung O und einer Primzahl p eine über F_p definierte elliptische Kurve E zu bestimmen, deren Endomorphismenring zu O isomorph ist. Die Komplexität und damit der Rechenaufwand der CM-Methode wird dabei von der Klassenzahl h(O) und der Diskriminante der Ordnung O bestimmt. Die Anwendung der CM-Methode wurde in den Dissertationen von A.-M. Spallek [IEM, 1994, preprint no. 18] und der Erfinderin A. Weng [IEM, 2002, preprint no. 11] auf die Konstruktion hyperelliptische Kurven mit Geschlecht 2 und Klassenzahl 1 (Spallek) bzw. auf hyperelliptische Kurven mit Geschlecht 2 und bis zu Klassenzahl 10, sowie Spezialfälle von hyperelliptischen Kurven vom Geschlecht 3 und höher ausgedehnt (Weng).

Insbesondere wird im erfindungsgemäßen Verfahren ein Repräsentantensystem aller Isomorphieklassen einfacher prinzipal polarisierter Abelscher Varietäten bestimmt. Die Aufzählung der Isomorphieklassen wird dabei vereinfacht, da nicht geprüft werden braucht, ob die Fundamentaleinheit eine relative Norm einer Einheit im CM-Körper K ist.

Ferner können die Periodenmatrizen in äquivalente Siegelreduzierte Matrizen transformiert und damit eine schnellere Konvergenz der Thetanullwerte erreicht werden.

In einer weiteren bevorzugten Ausführungsform wird die hyperelliptische Kurve über dem Körper C der komplexen Zahlen aus sechs von zehn errechneten Thetanullwerten bestimmt.

Weiterhin wird gemäss einer bevorzugten Variante des erfindungsgemäßen Verfahren eine Vielzahl, insbesondere mehr als hundert oder sogar mehr als tausend, von möglichen CM-Körpern bestimmt und die zu den CM-Körpern gehörenden Klassenpolynomen berechnet und als Datensatz vor der Anwendung des Verfahrens zur Bestimmung einer sicheren hyperelliptischen Kurve gespeichert.

In einer Variante des erfindungsgemäßen Verfahrens wird die Auswahl von möglichen CM-Körpern durch einen Test reduziert. Damit kann sichergestellt werden, dass für die Gruppenordnung eine exakte Primzahl erhalten werden kann.

Bevorzugterweise wird im erfindungsgemäßen Verfahren die dem endlichen Körper F_p zugrundeliegende Primzahl p so gewählt, dass das Minimalpolynom des CM-Körpers K über F_p in vier unterschiedliche Linearfaktoren zerfällt.

In einer weiteren Variante ist der der Kurve zugrundeliegende endliche Körper F_q nicht prim.

FIG.1 beschreibt einen ersten Teilschritt gemäss der Erfindung zur Bestimmung eines CM-Körpers und der zugehörigen Klassenpolynome;

FIG. 2 beschreibt einen zweiten Teilschritt gemäss der Erfindung zur Bestimmung einer kryptographisch-geeigneten Kurve.

Im folgenden werden Schritte des erfindungsgemäßen Verfahren im Detail beschrieben. Das Verfahren beinhaltet zwei Teilschritte. Der erste Teilschritt behandelt die Bestimmung eines CM-Körpers K, einer geeigneten Primzahl p zur Definition des Körpers F_p und einer geeigneten Gruppenordung n.

Zunächst wird ein geeigneter CM-Körper K bestimmt durch eine total imaginär quadratische Erweiterung eines total reellen Zahlkörpers K_0 mit Klassenzahl $h_{K0} = 1$. Ein solcher CM-Körper kann beispielsweise durch die Menge $K = Q(i(a + bd^{1/2})^{1/2})$ gegeben sein, wobei a, b und d ganze Zahlen sind.

Die Primzahl p wird so gewählt, dass die drei folgenden Bedingungen erfüllt sind:

1. Es existiert eine Zahl w aus O_K, so dass $w\underline{w} = p$ ist, wobei O_K die maximale Ordnung von K ist und $\underline{w}$ das komplex konjugierte Element von w. (Hier wie im folgenden kennzeichnet die Unterstreichung das komplex konjugierte Element der unterstrichenen Größe.)

2. Entweder ist $n_1 = \Pi(1 - w_i)$ oder $n_2 = \Pi(1 + w_i)$ fast prim, wobei sich das Produkt Π über alle Konjugierten w_i von w in K erstreckt.

3. Eine der Ordnungen n_i $(i = 1,2)$ ist von der Form kq, wobei k eine kleine Zahl ist und q eine Primzahl ist, die Bedingung die Bedingung erfüllt, dass die Ordnung von p in F_q groß ist.

Die Auswahl von p kann dabei vereinfacht werden, indem eine beliebige Zahl η aus O_K ausgewählt wird und geprüft wird, ob das Produkt $\eta\underline{\eta}$ mit ihrem komplex konjugiertem Element eine Primzahl ist. Wenn dies der Fall ist, können n_1 oder n_2 gemäss Bedingung 2 geprüft werden. Die Auswahl der Zahl η sollte dabei so erfolgen, dass sichergestellt wird, dass ihre relative Norm in der Menge Z der ganzen Zahlen liegt.

Alternativ kann eine beliebige Primzahl p aus Z gewählt werden und die Minimalpolynome in Z[x] von allen Lösungen der absoluten Normgleichung $N_{K/Q}(w) = p^2$ bestimmt werden. Aus diesen Minimalpolynomen werden diejenigen gewählt, die irreduzibel sind und Nullstellen mit dem Absolutwert $p^{1/2}$ haben. Diese Minimalpolynome werden dann an der Stelle x=1 ausgewertet. Daraus ergibt sich eine Menge S von möglichen Gruppenordnungen n_i . Diese Menge hat höchstens vier verschiedene Elemente. Diese Werte n_i können dann auf die obigen Bedingungen 1 und 2 getestet werden.

Für den folgenden zweiten Teilschritt kann angenommen werden, dass ein CM-Körper K, eine Primzahl p und eine Gruppenordnung n bestimmt wurden, die die Bedingungen 1-3 des ersten Teilschritts erfüllen. In diesem zweiten Teilschritt wird eine hyperelliptische Kurve über F_p konstruiert, die eine Divisorklassengruppe der Ordnung n aufweist.

Dabei wird für hyperelliptische Kurven vom Geschlecht 2 ausgenutzt, dass die Jacobischen Varietäten dieser Kurven genau die prinzipal polarisierten Abelschen Varietäten der Dimension 2 sind. Weiter lässt sich nach bekannten Methoden ein Repräsentantensystem aller Isomorphieklassen einfacher prinzipal polarisierten Abelschen Varietäten über dem Körper C der komplexen Zahlen finden, die eine komplexe Multiplikation mit O_K haben. Ebenso ist es im Prinzip bekannt, eine Periodenmatrix Ω dieser Varietäten aus der Menge H_2 zu bestimmen, wobei $H_2 = \{M$ aus $Gl_2(C)$, $M^t = M$, mit Im M positiv definit$\}$ die Siegelsche obere Halbebene der

Dimension 2 ist. Die Matrix ist somit symmetrisch und besitzt einen positiv definiten Imaginärteil.

Als Beispiel sei

$K_0 = Q(6^{1/2})$ mit $O_{K0} = Z + \omega Z$, $\omega = 6^{1/2}$

$K = Q(i(3 + 6^{1/2})^{1/2})$

$p = 1397033943070534673810094 1$ und

$n = 19517038380905957503092892071401185135497196423837 6$

Es wird $\eta = i(3 +)^{1/2})$ gesetzt. Dabei hat die Fundamentaleinheit ε_0 von $Q(6^{1/2})$ eine positive Norm. Dann wird ein Repräsentantensystem der Idealklassengruppe in einer relativen Ganzheitsbasis mit Bezug auf den reellen quadratischen Unterkörper O_{K0} dargestellt als:

$I_K = \{A_1 = O_K = O_{K0} + \eta\, O_{K0}, A_2 = (1 - 6^{1/2})\, O_{K0} + (-1 + \eta)\, O_{K0}\}$.

Aus der allgemeinen Darstellung von A_1 und A_2

$A_i = \alpha\, O_{K0} + \beta\, O_{K0}$

wird

$\tau_i = \alpha / \beta$ berechnet, wobei mit dem oben genannten Beispiel gilt:

$\tau_i = 0.42837299059613220 11i$

$\tau_2 = 0.22474487139158904\,90 + 0.52464762327529031\,78i$

Eine Einbettung σ von K in den Körper der komplexen Zahlen C ist gegeben durch

$\sigma\,(i\,(3 + 2^{1/2})^{1/2}) = -\,i\,(3 - 2^{1/2})^{1/2}$ und

ρ als dem dazu komplex konjugierten Element. Ein Repräsentantensystem aller Isomorphieklassen einfacher prinzipal polarisierten Abelschen Varietäten, die eine Multiplikation mit O_K haben, ist dann gegeben durch die Menge der Tupel

$\{ (\tau_1,\tau_1^{\sigma}),\ (\varepsilon_0\,\tau_1,(\varepsilon_0\,\tau_1)^{\sigma}),\ (\tau_1,\tau_1^{\rho\sigma}),\ (\varepsilon_0\,\tau_1,(\varepsilon_0\,\tau_1)^{\rho\sigma}) \}.$

Die zugehörige Periodenmatrix für ein Tupel (s_1,s_2) lautet

$$\Omega_{s1,s2} = \frac{1}{\omega - \omega^{\sigma}} \begin{pmatrix} \omega^2 s_1 - \omega^{\sigma 2} s_2 & \omega s_1 - \omega^{\sigma} s_2 \\ \omega s_1 - \omega^{\sigma} s_2 & s_1 - s_2 \end{pmatrix}.$$

Mit dem folgenden Schema werden die Isomorphieklassen abgezählt, wobei gelten soll, dass der Körper $K = Q(i(a + bd^{1/2})^{1/2})$ ein CM Körper, ε_0 die Fundamentaleinheit, σ die Konjugation

$\sigma\,(i\,(a + bd^{1/2})^{1/2}) = -\,i\,(a - bd^{1/2})^{1/2}$

und ρdie komplexe Konjugation ist. Für einen Repräsentanten $A_i = \alpha_i\,O_{K0} + \beta_i\,O_{K0}$ ergibt $\tau_i = \alpha_i / \beta_i$ mit $Im(\tau_i) > 0$. Mit $\{\tau_1,\ldots\ldots, \tau_k \ldots., \tau_{hk}\}$, $k<= h$ als Klassengruppe gilt: $Im\ \tau_i^{\sigma} > 0$ für $i <= k$ und $Im\ \tau_i^{\sigma} < 0$ für $i > k$. Die folgenden Regeln erlauben es, eine geeignete Menge S von Repräsentanten von einfachen prinzipal polarisierten Abelschen Varietäten mit komplexer Multiplikation mit O_K zu bestimmen:

Wenn K Galois, dann $S := \{ (\tau_i, \tau_i^{\sigma}),\ 1<=i<=h \}$.

Wenn K nicht-normal ist und wenn $N(\varepsilon_0) = 1$ dann $k := h/2$;
$S := \{ (\tau_i, \tau_i^{\sigma}),(\varepsilon_0\tau_i, (\varepsilon_0\tau_i)^{\sigma}), 1<=i<=k \} \cup \{ (\tau_i, \tau_i^{\rho\sigma}),(\varepsilon_0\tau_i, (\varepsilon_0\tau_i)^{\rho\sigma}), k+1<=i<=2k \}$ und

wenn K nicht-normal ist, aber $N(\varepsilon_0) = -1$ dann lässt sich definieren:

$$S := \{ (\tau_i, \tau_i^{\sigma}),(\varepsilon_0\tau_i, (\varepsilon_0\tau_i)^{\rho\sigma}), 1<=i<=h \}.$$

Für jede der oben bestimmten Periodenmatrix Ω_i mit $i = 1, ..., 4$ werden dann die absoluten Invarianten $j_k^{(i)}$ mit $k = 1, 2, 3$ errechnet. Dazu werden für jede Matrix Ω_i zunächst die geraden Thetanullwerte errechnet und mit Hilfe der Thetanullwerte diejenige Kurve über C bestimmt,deren Jacobi Varietät der Periodenmatrix Ω entspricht. Aus den absoluten Invarianten werden die Klassenpolynome der Kurve berechnet.

Die geraden Thetanullwerte einer Periodenmatrix Ω_i sind gegeben durch

$$\theta\begin{bmatrix}\delta\\ \varepsilon\end{bmatrix}(\Omega_i) = \sum_{n \text{ aus } Z^g} \exp(\pi i((n+1/2\,\delta)^t\Omega_i(n+1/2\delta)+2(n+1/2\delta)(z+1/2\varepsilon)^t)),$$

mit δ, ε aus der Menge $\{0,1\}^g$, $\delta^t\,\varepsilon = 0 \bmod 2$.

Für Kurven des Geschlechts 2 ergeben sich aus dieser Funktion genau zehn gerade Thetanullwerte. Die Güte der Näherung sollte so gewählt werden, dass die Approximation der im weiteren berechneten Klassenpolynome ausreicht, um in Z[1/n][X] mit einer glatten Zahl n zu liegen. Im beschriebenen Beispiel reichen 70 Dezimalstellen aus.

Die Konvergenz der Gleichung auf die Thetanullwerte lässt sich verbessern, wenn an Stelle der Matrizen Ω_i aus H_2 Siegel-reduzierte Matrizen Ω' in die Funktion eingesetzt werden. Eine Matrix $\Omega' = X + iY$ aus H2 mit $X = (x_{kl})$ und Indizes $k,l = \{1,2\}$ ist

Siegel-reduziert, wenn gilt

1. $1/2 <= x_{kl} <= -1/2$

2. Y is Minkowski reduziert

3. $|\det(CZ + D)| >= 1$ für alle $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp(4, Z)$

Mit Hilfe der Thetanullwerte lässt sich ein Modell der gesuchten Kurve über C bestimmen. Ein solches Modell ist das Rosenhain Modell

$y^2 = x(x-1) \Pi (x - \lambda_i)$,

wobei der Index i von 1 bis 2g-1 läuft, also für Kurven vom Geschlecht 2 bis 3. Das Rosenhain Modell erlaubt es, aus den Thetanullwerten die Werte λ_i zu berechnen . Im vorliegenden Beispiel sind

$\lambda_1 = 3.776147667954230524321 5 + 1.091914104240337886485 0i$

$\lambda_2 = \underline{\lambda_1}$

$\lambda_3 = - 0.5826628324044744213034$

Aus den 10 geraden Nullwerten ergeben sich auch die sogenannten absoluten Igusa Invarianten j_1, j_2, j_3 als bekannte Funktionen.

Sowohl die λ_i des Rosenhainmodells als auch die Igusa-Invarianten lassen sich jedoch aus lediglich sechs Thetanullwerten bestimmen:

$$\alpha_1 = \theta \begin{bmatrix} (00) \\ (10) \end{bmatrix} \quad \alpha_2 = \theta \begin{bmatrix} (01) \\ (10) \end{bmatrix} \quad \alpha_3 = \theta \begin{bmatrix} (11) \\ (10) \end{bmatrix}$$

$$\alpha_4 = \theta \begin{bmatrix} (00) \\ (10) \end{bmatrix} \quad \alpha_5 = \theta \begin{bmatrix} (01) \\ (10) \end{bmatrix} \quad \alpha_6 = \theta \begin{bmatrix} (11) \\ (10) \end{bmatrix}$$

Die λ_i des Modells

$f(x) = x(x-1)(x - \lambda_3\ )\ (x - \lambda_3\ )\ (x - \lambda_5\ )$ sind gegeben durch:

$$\lambda_3 \ = - \alpha_1^{\ 2}\alpha_2^{\ 2}\ (\alpha_3^{\ 2}\alpha_4^{\ 2})^{-1}$$

$$\lambda_3 \ = - \alpha_5^{\ 2}\alpha_2^{\ 2}\ (\alpha_3^{\ 2}\alpha_6^{\ 2})^{-1}$$

$$\lambda_3 \ = - \alpha_5^{\ 2}\alpha_1^{\ 2}\ (\alpha_4^{\ 2}\alpha_6^{\ 2})^{-1}$$

und die (nicht-absoluten) Igusa-Invarianten werden beschrieben durch

$I_2 = - 120A'$, $I_4 = - 720\ (A')^2 + 6750\ B'$,
$I_6 = 8640(A')^3 - 108000A'B' + 202500C'$..

mit

$A' = (f, f)_6$, $B' = (i, i)_4$., $C' = (i, \Delta)_6$ und
$i = (f, f)_4$, $\Delta = (i, if)_2$

wobei die Notation $(gh)_k$ die Überschiebung zweier Binärformen g und h vom Grad n und m der Form

$$(gh)_k = \frac{(m-k)!(n-k)!}{m!n!} \left(\frac{\delta g}{\delta x} \frac{\delta h}{\delta z} - \frac{\delta g}{\delta z} \frac{\delta h}{\delta x} \right)^k$$

darstellt. Aus den Igusa-Invarianten ergeben sich dann die absoluten Invarianten:

$j_1 = I_2\, I_4^2 / \Delta$, $j_2 = I_2^3\, I_4 / \Delta$, $j_3 = I_4\, I_6 / \Delta$.

Die Berechnung der Igusa-Invarianten lässt sich weiter beschleunigen durch eine Sortierung der Klassengruppe I_K der Idealklassen nach Paaren von Idealklassen und deren Inversen. Da im Körper K_0 mit Klassenzahl 1 gilt, dass die inversen Idealklassen gleich den komplex konjugierten Idealklassen ist, braucht für jedes gefundene Paar von komplex konjugierten Idealklassen nur eine einfache prinzipal polarisierten Abelschen Varietät berechnet werden:

Wenn (τ_1, τ_1^{Ψ}) die zu dem Ideal A_i und CM-Typ (K,ψ) gehörende prinzipal polarisierten Abelschen Varietät ist, dann repräsentiert $(-\underline{\tau}_1, -\underline{\tau}_1^{\Psi})$ die zu $\underline{A_i}$ gehörende prinzipal polarisierten Abelschen Varietät des gleichen CM-Typs. Wenn weiter j_i die Igusa-Invariante von (τ_i, τ_i^{Ψ}) ist, dann ist die entsprechende Igusa-Invariante von $(-\underline{\tau}_i, -\underline{\tau}_i^{\Psi})$ gleich $\underline{j_i}$. Also braucht für jedes Inversenpaar von komplex konjugierten Idealklassen lediglich eine Igusa-Invariante bestimmt zu werden. Der Rechenaufwand für diesen Schritt halbiert sich folglich nahezu.

Die Klassenpolynome H_k lassen sich darstellen als Funktionen der Igusa-Invarianten j_k, $k = 1,\ldots,3$:

$H_k(X) := \Pi\, (X-j_k^{(i)})$ mit $i = 1, \ldots, 4$

Die Polynome liegen im Körper der rationalen Polynome Q[x]. Durch Anwendung des Kettenbruchverfahrens und anschließender Multiplikation lässt sich $H_k(X)$ in ein ganzzahliges Polynom $H_k(X)^{\#}$ umwandeln. Im Beispiel erhält man für

$$H_1(X) = \Pi\, (X- j_1^{(i)})$$
$$= \quad -46989351758.431801106481797\, X^3$$
$$-459701468131471 29.294447100607881\, X^2$$

$$+ 1092445938154906930400 9.2889829929649614 0\, X$$
$$+ 6266220289945366250119527 3.54688887371081210299.$$

Falls die Genauigkeit hinreichend hoch gewählt wurde, wird mit dem Kettenbruchalgorithmus das kleinste gemeinsame Vielfache der Nenner der Koeffizienten gefunden. Im vorliegenden Beispiel ist dies 11^4. Daraus ergibt sich das ganzzahlige Polynom:

$$H_1(X)^{\#} = 14641\, X^4 - 687971099095200\, X^3 - 6730489194912871200000\, X^2$$
$$- 1599450098052599236800000 00\, X$$
$$+ 917437312650901072680000000000.$$

Die Klassenpolynome der Form $H_k(X)$ über $Q[x]$ und der Form $H_k(X)^{\#}$ über dem Körper der ganzzahligen Polynome $Z[x]$ hängen nur von der Wahl des CM-Körpers K ab. Der zugrundeliegende Primzahlkörper F_p für die hyperelliptische Kurve kann jedoch auch nach Festlegung des CM-Körpers K noch variieren. Es ist daher vorteilhaft, geeignete CM-Körper und die dazugehörigen Klassenpolynome in grosser Zahl, praktischerweise hunderte oder tausende, im voraus zu berechnen und in geeigneter Weise zu speichern. Ist nach diesem Schritt die Erzeugung einer hyperelliptischen Kurve für die Anwendung einer Verschlüsselung erforderlich, kann auf einen zufällig ausgewählten CM-Körper, beziehungsweise zufällig ausgewählte Klassenpolynome aus der abgespeicherten Datei zugegriffen werden und nach den im ersten Teilschritt aufgeführten Kriterien eine geeignete Primzahl p und Gruppenordnung n bestimmt werden. Danach können direkt die folgenden Schritte zur Bestimmung der hyperelliptischen Kurve über F_p durchgeführt werden, ohne die Klassenpolynome neu zu bestimmen.

Ferner kann es für die Implementierung eines kryptographischen Protokolls vorteilhaft sein, sich auf Gruppenordnungen zu beschränken, die exakt prim sind.

Dazu wird vorgeschlagen, die Auswahl des CM-Körper zu beschränken und nur solche CM-Körper K zu verwenden, für die das Minimalpolynom K/Q modulo 2 zwei

verschiedene Faktoren hat oder irreduzible ist.

Für die folgenden Schritte zur Berechnung der hyperelliptischen Kurve über F_p wird also davon ausgegangen, dass der CM-Körper K festgelegt ist und die Klassenpolynome $H_k(X)^\#$ entweder den oben beschriebenen Schritten folgend berechnet wurden oder einer vorausberechneten Datei entnommen wurden.

Als nächster Schritt wird die Kurve berechnet. Dazu werden für jedes Tripel (a_1, a_2, a_3) aus $(F_p)^3$ mit $H_k(X)^\#(a_k) = 0 \bmod p$ die folgenden Schritte durchlaufen:

Setze $j_1 := a_1$, $j_2 := a_2$, $j_3 := a_3$. Berechne dann aus j_i die Mestre Invarianten A_{ij} und H_{ijk}. Nach dem bekannten Mestre Verfahren über endlichen Körpern, wie beispielsweise in J.-F. Mestre, „Construction des courbes de genre 2 a partir de leurs modules", Progr. Math., Birkhäuser, 94:313-334, 1991 beschrieben, sind die Mestre Invarianten Koeffizienten einer Quadrik der Form

$$\Sigma A_{ij} x_i x_j$$

und einer Kubik der Form

$$\Sigma H_{ijk} x_i x_j x_k$$ wobei die Summation über die Indizes i, j, k von 1 bis 3 läuft

Aus einer Parametrisierung der Quadrik durch Polynome $f_1(t)$, $f_2(t)$, $f_3(t)$ und deren Einsetzung in die Kubik

$$\Sigma H_{ijk} f_i(t) f_j(t) f_k(t)$$

lässt sich ein Modell

$$y^2 = f(t)$$

der hyperelliptischen Kurve über F_p erhalten. Durch projektive Transformation lässt sich der Grad des Polynoms f(t) (im Allgemeinen 6) dann um 1 auf 5 verringern, wenn f(t) eine Nullstelle in F_p besitzt. Danach prüfe durch zufällige Wahl eines Divisors D

und unter Bildung des Produktes nD, ob die Divisorklassengruppe der Kurve Ordnung n hat.

Die aus dem angeführten Beispiel resultierende Kurve lautet

$$y^2 = x^5 + 4464505615838997835224600\ x^4 + 1194299411533922924046961 4\ x^3 + 1108584063993749350888007\ x^2 + 1145734473666435422023499\ x + 2901066642986978406675671$$

und ist über den Körper F_p definiert wobei

$p = 13970339430705346738100941$ und

$n = 195170383809059575030928920714011851354971964238376$

gleich den oben erwähnten Werten ist. Der Wert für n das 152-fache einer Primzahl.

Der Mestre-Algorithmus kann durch eine geeignete Wahl der Primzahl p beschleunigt werden. Voraussetzung dafür ist, dass der CM-Körper K nicht-normal ist und p aus der Menge der ganzen Zahlen Z eine Primzahl ist, die sich vollständig in K zerlegt oder, äquivalent dazu, sich das Minimalpolynom von K in F_p in vier unterschiedliche Linearfaktoren zerlegen lässt. Unter dieser Voraussetzung halbiert sich die Zahl der Linearfaktoren modulo p für jedes Klassenpolynom, sofern die obige Gleichung $w\underline{w} = p$ bis auf das Vorzeichen und das konjugiert komplexe Element nur eine Lösung w aus der Menge O_K besitzt. Diese Halbierung der Linearfaktoren beschleunigt die Anwendung des Mestre-Algorithmus um das Achtfache.

Um diesen Vorteil auszunutzen, wird geprüft, ob eine im obigen ersten Teilschritt bestimmte Primzahl p das Minimalpolynom von K in F_p in vier unterschiedliche Linearfaktoren zerlegt. Dies kann durch direkte Berechnung geschehen. Wenn p jedoch,

wie oben beschrieben, durch Auswertung an der Stelle x=1 von Minimalpolynomen in Z[x] gewählt wurde, die irreduzibel sind und die Nullstellen mit dem Absolutwert $p^{(1/2)}$ haben, sind die gefunden Primzahlen bereits vorsortiert. Danach lassen sich die Primzahlen auf solche beschränken, die lediglich zwei verschiedene Gruppenordnungen zulassen.

Wenn der CM-Körper zyklisch ist und der Exponent der Idealklassengruppe größer als zwei ist, dann haben die in diesem Sinne vorteilhaften Primzahlen eine positive Dichte. Insbesondere gibt es unendliche viele dieser Primzahlen.

Das beschriebene Verfahren zur Erzeugung einer für kryptographische Anwendungen geeignete hyperelliptische Kurve kann auf nicht prime endliche Körper F_q erweitert werden. Die Zahl $q := p^f$ ist dabei definiert als Potenz einer Primzahl p. Der Exponent f ist eine natürliche Zahl und wird als Erweiterungsgrad bezeichnet. Es kann ferner angenommen werden, dass die Kurve nicht über einem Unterkörper von F_q definierbar ist.

Für den Fall, dass der CM-Körper K Galoissch ist, sollte p so gewählt werden, dass

$p = A\underline{A}$ in K/K_0 .

Wenn f minimal gewählt wird mit der Bedingung, dass

$A^f = (w)$, mit w Element aus O_K

ein Hauptideal ist, dann existiert eine Wurzel der Klassenpolynome über F_q Aus diesen Wurzeln können wie oben angegeben mittels des Mestre-Algorithmus hyperelliptische Kurven über F_q konstruiert werden. Die Ordnung dieser Kurven ist gegeben durch

$n = \Pi\ (1 - w_i)$ oder $\Pi\ (1 + w_i)$ wobei der Index $i = 1,\ldots,4$ und w_i das komplex

konjugierte Element von w ist.

Für den Fall, dass der CM-Körper nicht Galoissch oder nicht-normal ist, sollte die Primzahl p so gewählt werden, dass das Primideal (p) in drei Ideale zerfällt:

$(p) = p_1\underline{p_2}p_2.$

Dann gibt es ein Ideal A, so dass

$A = p_1p_2^2$

ist und f wieder minimal gewählt mit

$A^f = (w)$, mit w Element aus O_K.

Unter diesen Bedingungen können wie oben angeben mittels des Mestre-Algorithmus hyperelliptische Kurven über dem nicht-primen endlichen Körper F_q konstruiert werden, wobei $q = p^{2f}$ ist. Die Gruppenordnung kann wie im Fall eines Galoisschen Körpers K berechnet werden.

Als Beispiel wird ausgehend von einem CM-Körpers K mit der Klassengrad $h_K = 5$ eine Kurve über einem Körper des Erweiterungsgrad $f = 2\ h_K = 10$ erzeugt. Als Primzahl dient $p = 911$, dessen Ideal (p) über dem Körper K in drei Primideale zerfällt. Für das Ideal $A = p_1p_2^2$ gilt, dass $f = 5$ der kleinste Exponent ist. Daher ist A^f Hauptideal.

Die Elemente in F_q mit $q = 911^{10}$ lassen sich durch Polynome vom Grad 9 angeben. Die modulo p irreduziblen Klassenpolynome sind

$$H_1(X) = 701X^{10} + 401X^9 + 322X^8 + 712X^7 + 125X^6 + 774X^5 + 513X^4 + 869X^3 + 474X^2 + 49X + 680 \bmod p$$

$$H_2(X) = 186X^{10} + 895X^9 + 453X^8 + 86X^7 + 180X^6 + 47X^5 + 811X^4 + 339X^3 + 887X^2 + 296X + 371 \bmod p$$

$$H_3(X) = 75X^{10} + 280X^9 + 616X^8 + 737X^7 + 511X^6 + 179X^5 + 623X^4 + 533X^3 + 616X^2 + 697X + 700 \bmod p$$

Es ergeben sich zwei mögliche Gruppenordnungen

n_1= 155012792308846128138632814006095268154658315370266774539376

n_2 =
155012792308846046374979954330693046736810307187589966188400

Die zugehörige Kurve $y^2 = f(x)$ lautet

$$\begin{aligned} f(x) = x^5 &+ [9\ \ 703\ \ 722\ \ 261\ \ 507\ \ 119\ \ 164\ \ 322\ \ 684\ \ 741]\ x^4 \\ &+ [715\ \ 508\ \ 396\ \ 153\ \ 661\ \ 164\ \ 513\ \ 167\ \ 892\ \ 156]\ x^3 \\ &+ [548\ \ 810\ \ 311\ \ 54\ \ 483\ \ 636\ \ 130\ \ 899\ \ 845\ \ 101]\ x^2 \\ &+ [550\ \ 294\ \ 663\ \ 157\ \ 288\ \ 697\ \ 710\ \ 60\ \ 475\ \ 608]\ x \\ &+ [301\ \ 385\ \ 355\ \ 533\ \ 347\ \ 763\ \ 659\ \ 163\ \ 720\ \ 665], \end{aligned}$$

wobei die verkürzende Notation

$$a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \ldots + a_8 z^8 + a_9 z^9 = [a_0\ \ a_1\ \ a_2\ \ a_3\ \ldots\ a_8\ \ a_9]$$

verwendet wurde.

Die Gruppenordnung ist $n_2 = 400r$, wobei r eine Primzahl mit 57 Dezimalstellen ist.

PATENTANSPRÜCHE

1. Verfahren zur Bestimmung einer kryptographisch-geeigneten hyperelliptische Kurve mit den Schritten:

- Auswahl eines CM-Körpers K;
- Bestimmung eines Repräsentantensystem aller Isomorphieklassen einfacher prinzipal polarisierten Abelschen Varietäten mit komplexer Multiplikation mit der maximalen Ordnung in K;
- Bestimmung von zum Repräsentantensystem zugehörigen Periodenmatrizen;
- Bestimmung von Thetanullwerten;
- Bestimmung von Klassenpolynomen des CM-Körpers über einem endlichen Körper F_q;;
- Bestimmung einer hyperelliptischen Kurve über dem endlichen Körper F_q und
- Festlegung der Gruppenordnung n der Divisorklassengruppe der hyperelliptischen Kurve.

2. Das Verfahren nach Anspruch 1, wobei die hyperelliptische Kurve vom Geschlecht 2 ist.

3. Das Verfahren nach Anspruch 1, wobei aus den Thetanullwerten Igusa-Invarianten bestimmt werden.

4. Das Verfahren nach Anspruch 3, wobei die Igusa-Invarianten verwendet werden, um die Klassenpolynome zu bestimmt.

5. Das Verfahren nach Anspruch 1, wobei aus den Thetanullwerten Mestre-Invarianten bestimmt werden.

6. Das Verfahren nach Anspruch 5, wobei das Mestre-Verfahren zur Erzeugung der hyperelliptischen Kurve über F_q verwendet werden.

7. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei eine Vielzahl von geeigneten CM-Körpern K und die zugehörigen Klassenpolynome in zugreifbarer Form gespeichert werden und zur Bestimmung der hyperelliptischen Kurve ein CM-Körper aus der gespeicherten Vielzahl ausgewählt wird.

8. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei die Periodenmatrizen in Siegel-reduzierter Form verwendet werden.

9. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei nur sechs Thetanullwerte bestimmt werden.

10. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei zur Bestimmung des Repräsentantensystem nicht getestet wird, ob die Fundamentaleinheit des reellen Teilkörper des CM-Körpers K die Norm einer Einheit des CM-Körpers ist.

11. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei zur Bestimmung des Repräsentantensystem eine Menge von Idealklassen bestimmt wird.

12. Das Verfahren nach Anspruch 11, wobei Paare von zueinander inversen Idealklassen identifiziert werden und für jedes Paar Igusa-Varianten nur einmal aus den Thetanullwerten bestimmt werden.

13. Verfahren nach einem der vorhergehenden Ansprüche, wobei q eine Primzahl p ist.

14. Verfahren nach Anspruch 13, wobei die Primzahl p so gewählt wird, dass jedes Klassenpolynom höchstens h_K Linearfaktoren aufweist, wobei h_K die Klassenzahl des CM-Körpers K ist.

15. Verfahren nach einem der vorhergehenden Ansprüche, wobei der CM-Körper so gewählt wird, dass die Gruppenordnung n der Divisorklassengruppe der hyperelliptischen Kurve exakt prim wird.

16. Verfahren nach einem der vorhergehenden Ansprüche, wobei q die Potenz einer Primzahl p ist.

17. Kryptographisches Verfahren, wobei Schlüssel zum Verschlüsseln von Daten aus der Gruppe der F_q-rationalen Zahlen einer hyperelliptischen Kurve bestimmt werden, die nach Verfahren gemäss einem der vorhergehenden Ansprüche erzeugt wurde.

ZUSAMMENFASSUNG

Verfahren zur Konstruktion kryptographisch geeigneter hyperelliptischer Kurven

Um ein Verfahren zur schnellen Bestimmung sicherer hyperelliptischer Kurven zu schaffen, wird vorgesehen, dass geeignete hyperelliptische Kurven unter Verwendung der Methode der komplexen Multiplikation konstruiert werden. Das erfinderische Verfahren erzeugt für kryptographische Anwendungen geeignete hyperelliptische Kurven vom Geschlecht 2 über endlichen Körpern mit großer Charakteristik.

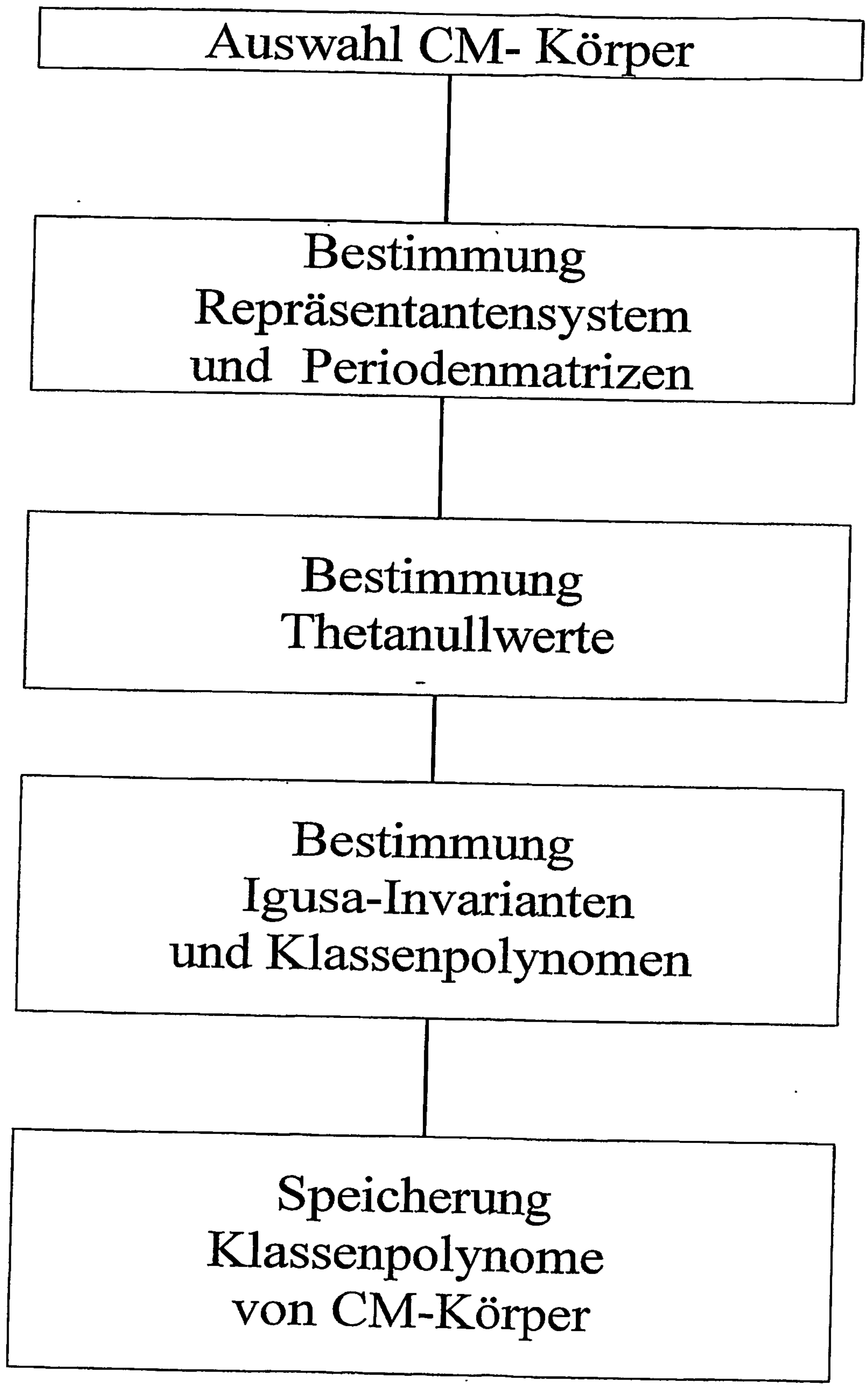
Auswahl CM- Körper
Bestimmung Repräsentantensystem und Periodenmatrizen
Bestimmung Thetanullwerte
Bestimmung Igusa-Invarianten und Klassenpolynomen
Speicherung Klassenpolynome von CM-Körper

Fig.1

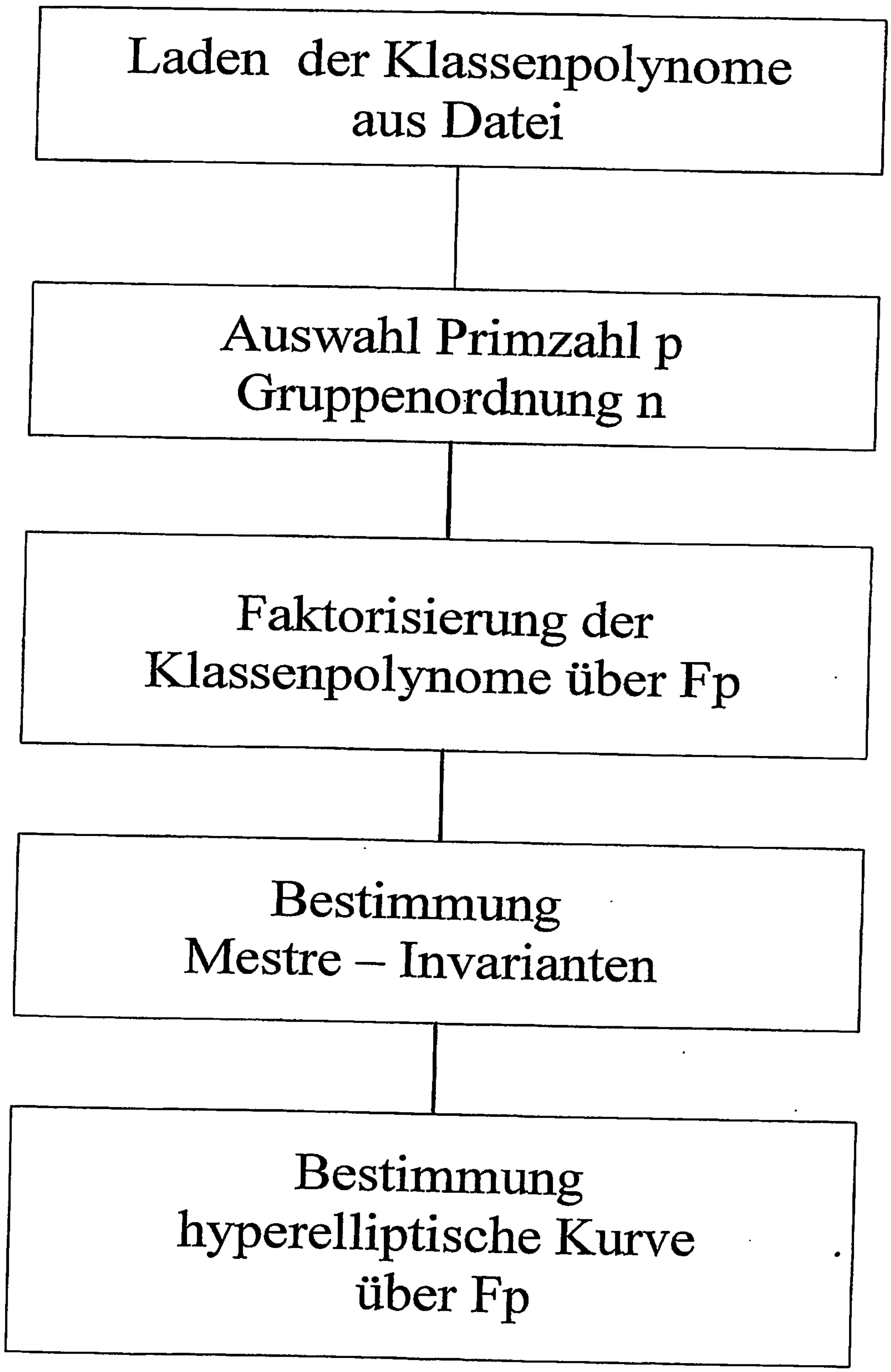
Laden der Klassenpolynome aus Datei
Auswahl Primzahl p
Gruppenordnung n
Faktorisierung der Klassenpolynome über Fp
Bestimmung Mestre – Invarianten
Bestimmung hyperelliptische Kurve über Fp

Fig.2